# Bluesocket BlueSecure Access Point (BSAP) FAQ

**Updated 11/07/2011**

### 20MB space error when attempting to upload AP firmware to the BSC

When attempting to upload AP firmware to the BSC under wireless>firmware the following error may be received:

"Only 20MB of space is available for upload"

The BSC has 20 MB of space allocated for AP firmware. If the above error is received perform the following:

1. Delete the previous version of AP firmware under wireless>firmware BEFORE attempting to upload new AP firmware.

2. Delete any un-used firmware. For example the BSC software image includes BSAP-1800v2/1840 and BSAP-1800v1 AP firmware. Perhaps you only have BSAP-15XXs. If so you could delete the 18XX firmware to make room for the BSAP-15XX Firmware

3. If you have more than 2 BSAP model types you may be required to swap AP firmware as needed when bringing up new BSAPs for the first time or alternatively configure the BSC to store AP firmware on a TFTP server external to the BSC.

---

### BSAP-1800v2 is showing up as a BSAP-1840 under wireless>AP in the BSC.

BSAP-1800v2 require a minimum of 6.5.0.8 bluepatch version 1 and ap firmware 6.5.0-15. Both are available for download along with release notes at support.bluesocket.com. If you installed the BSAP-1800v2 without bluepatch version 1 or 6.5.0-15 they will be recognized as BSAP-1840's. After applying BP1 and 6.5.0.15 ap firmware delete the aps from wireless>ap. They should rediscover as 1800v2.

---

### Can I use the AC power adapter from a BSAP-1500/1540/1700/1800v1 to power a BSAP-1800v2/1840?

NO. The BSAP-1500/1540/1700/1800v1 all require 48 volt AC power adapters. The BSAP-1800v2 requires a 12 volt DC power adapter (Part Number BSAP-PWR-12v-00-0). Using a legacy power adapter will provide irreversible damage to the product that will void the hardware

warranty.

---

**Does the AP or the BSC's managed interface have to be on a trunk port allowing the appropriate vlans? This may be referred to as tagging vlans on some switches.**

**BlueSecure Access Points**
By default BSAPs tunnel traffic back to the BSC in EtherIP (IP Protocol 97). The 802.1q vlan tagging is performed inside the tunnel and not exposed to the switch. If you are using BlueSecure access points you are not required to put the BSAPs or the BSC's managed interface on trunk ports. They can be placed on access ports. This may be referred to as untagged ports on some switches. The exception to this is the BSAP-1600. BSAP-1600s do not support EtherIP tunneling.

**3rd Party Access Points**
If you are using 3rd party access points and you want to deploy multiple ssid assigned to multiple managed side vlans both the 3rd party access points and the BSC's managed interface must be placed on trunk ports. This may be referred to as tagging vlans on some switches. Here is an example vlan setup with the BSC, 3rd Party AP and Cisco switches.

-BSC's protected physical interface on vlan 5. This could be the existing wired network or a dmz.
-BSC's managed physical interface on vlan 10. Vlan 10 is used for 3rd party AP management in this example.
-Employee ssid assigned to managed vlan 15
-Guest ssid assigned to managed vlan 20

**BSC's Protected Interface Switchport Configuration**
Switchport mode access vlan 5

**BSC's Managed Interface Switchport Configuration**
Switchport mode trunk
Switchport trunk encapsulation dot1q
Switchport trunk allowed vlan 10,15,20
Switchport trunk native vlan 10

**3rd Party APs switchport Configuration**
Switchport mode trunk
Switchport trunk encapsulation dot1q
Switchport trunk allowed vlan 10,15,20
Switchport trunk native vlan 10

*****The physical interfaces of the BSC cannot send or receive dot1q tags, only the vlan interfaces can. Notice above the protected physical interface is on an access port (untagged) and the managed physical interface is on the native vlan of the trunk (untagged).**

Here is the same example vlan setup with HP switches.

vlan 5
untagged e10
vlan 10
untagged e11,e12
vlan 15
tagged e11,e12
vlan 20
tagged e11,e12

This example assumes the BSC's Protected interface is plugged into switchport e10, Managed interface into e11, and 3rd Party AP into e12.

*****Notice the protected physical and managed physical interfaces are untagged and the managed vlan interfaces are tagged. The physical interfaces of the BSC cannot send or receive dot1q tags, only the vlan interfaces can.**

**Wired Support**
If you are required to support wired users on the BSC you may be required to put the BSC's managed interface on a trunk port also. For example you may have a conference room where you could assign switchports to the guest vlan 15 so that visitors can get the BSC's login page and be policed by the BSC's role based authorization. If the wired users were placed on the managed physical network trunking/tagging would not be required.

**Edge-to-Edge**
The Edge-to-Edge feature essentially disables the EtherIP tunnel from the BSAP to the BSC on a per ssid basis. Therefore you may be required to put the BSAP and the managed physical interface on trunk ports if you are using the Edge-to-Edge feature. If the Edge-to-Edge ssid is assigned to the managed physical network (vlan 0) then trunking/tagging would not be required.

---

**I am setting up Internal 802.1x Authentication on the BSC. The BSC is configured to proxy to RADIUS. Do I need to configure a RADIUS client in the RADIUS server for every single access point or just the BSC?**

With internal 802.1x both BSAPs and 3rd Party APs are configured to send RADIUS requests to the BSC. The BSC is the RADIUS server and terminates EAP. The BSC then proxies inner methods i.e. PAP, CHAP, MSCHAP, MSCHAPv2 to the external RADIUS server. All RADIUS requests are sourced by the BSC's protected interface IP address and therefore you are not required to configure a RADIUS client in the RADIUS server for every single AP. You only need to configure a RADIUS client in the RADIUS server for the BSC with the protected interface IP address or DNS name.

---

**I am setting up Transparent 802.1x Authentication on the BSC. Do I need to configure a RADIUS client in the RADIUS server for every single access point or just the BSC?**

With Transparent 802.1x both BSAPs and 3rd Party APs are configured to send RADIUS requests to the RADIUS server. BSAPs however tunnel these requests in EtherIP (IP Protocol 97) to the BSC and the BSC then forwards them on to the RADIUS server. All RADIUS requests from the BSAPs are sourced by the BSC's protected interface IP address and therefore you are not required to configure a RADIUS client in the RADIUS server for every single BSAP. You only need to configure a RADIUS client in the RADIUS server for the BSC with the protected interface IP address or DNS name.

3rd Party access points however do not tunnel RADIUS request to the BSC and therefore you are required to configure a RADIUS client in the RADIUS server for every single 3rd Party AP. Alternatively configure a RADIUS client in the RADIUS server for the 3rd Party APs with an IP range.

---

**I am setting up Internal 802.1x Authentication on the vWLAN. The vWLAN is configured to proxy to RADIUS. Do I need to configure a RADIUS client in the RADIUS server for every single access point or just the vWLAN?**

With internal 802.1x BSAPs are configured to send RADIUS requests to the vWLAN. The vWLAN is the RADIUS server and terminates EAP. The vWLAN then proxies inner methods i.e. PAP, CHAP, MSCHAP, MSCHAPv2 to the external RADIUS server. All RADIUS requests are sourced by the vWLAN's network interface IP address and therefore you are not required to configure a RADIUS client in the RADIUS server for every single AP. You only need to configure a RADIUS client in the RADIUS server for the vWLAN with the network interface IP address or DNS name.

---

**I am setting up RADIUS-802.1x Authentication on the vWLAN. Do I need to configure a RADIUS client in the RADIUS server for every single access point or just the vWLAN?**

With RADIUS-802.1x BSAPs are configured to send RADIUS requests to the RADIUS server and therefore you are required to configure a RADIUS client in the RADIUS server for every single BSAP. Alternatively configure a RADIUS client in the RADIUS server with an IP range.

---

**I am trying to connect to the serial console port of the BSAP-1800v2/1840 but I am not receiving a response or I am receiving garbled characters.**

Check to make sure your terminal emulation program is set to 115200 Bits per second.

---

**My BSAP-1600 is not discovering the BSC. It is not showing up under wireless>AP in the BSC and I do not see the BSAP-1600 in the create new AP drop down.**

The BSAP-1600 is an autonomous access point. It is not a thin access point managed by the BSC. It is configured via it's own web based administrative console and or CLI.

---

**Obtaining 14 Digit Product Serial Numbers of BSC, BSAP, BVMS, and vWLAN**

**BlueSecure Controller (BSC)**
-In the web based administrative console go to Maintenance>Upgrade
-It may be necessary to read the serial number off of the physical hardware if you are unable to access the web based administrative console or the serial number is not displayed under Maintenance>Upgrade.

**BlueView Management System (BVMS)**
-Read the serial number off of the physical hardware as it is not available electronically.

**BlueSecure Access Points (BSAP)**

**BSAP-15XX, BSAP-1600, and BSAP-1700**
-Read the serial number off of the physical hardware as it is not available electronically.

**BSAP-18XX**
-In the web based administrative console of the BSC go to Wireless>AP. The serial number is located in the serial number column. If the serial number column is not displayed it may be necessary to scroll to the right to click customize to add the serial number column.
-In the web based administrative console of the vWLAN go to Provision>Wireless>AP. The serial number is located in the serial number column. If the serial number column is not displayed it may be necessary to scroll to the right to click customize to add the serial number column.
-It may be necessary to read the serial number off of the physical hardware if the BSAP-18XX has not yet discovered the BSC or the vWLAN. Alternatively the serial number can be obtained remotely via SSH. SSH to the ip address of the BSAP-18XX using port 2335. The default username/password is adm1n/blue1socket. Choose the option for Show Version Information from the console.

**Virtual Wireless Lan (vWLAN**)
-In the web based administrative console go to Platform>Maintain>Upgrade
-It may be necessary to read the serial number off of the physical hardware if you are unable to access the web based administrative console or the serial number is not displayed under Maintenance>Upgrade.

---

**Obtaining Software/Firmware and Patch versions of BSC, BSAP, BVMS, and vWLAN**

**BSC Software**
-In the web based administrative console Go to Maintenance>Upgrade and look for Current Version

**BSC Patches**
-In the web based administrative console go to Maintenance>Patch. Under Installed patches you will find a list of patches installed.

**BVMS Software**
-In the web based administrative console go to BlueView>upgrade. Under Current Partition Information look for the version.
**BVMS Patches**
-In the web based administrative console go to BlueView>Patch. Under Installed patches you will find a list of patches installed.

**vWLAN Software**
-In the web based administrative console go to Platform>Maintain>Upgrade and look for Current Version
**vWLAN Patches**
-In the web based administrative console go to Platform>Maintain>Patch. Under Installed patches you will find a list of patches installed.

**BSAP Firmware**
-If connected to BSC go to Wireless>AP and look in the firmware column in the BSC¿s web based administrative console
-If connected to vWLAN go to Provision>Wireless>AP and look in the firmware column in the vWLAN¿s web based administrative console
-If not yet connected to BSC or vWLAN connect to the serial console or ssh to the BSAP. Choose show version information from the console menu. See Salesforce solutions for how to connect to serial console or ssh to the BSAP.

---

**What 3rd party external antennas would Bluesocket recommend for use with the BSAP-1840?**

Mars 2.4Ghz or 5Ghz 5dBi Wide Beam 120 degree directional MIMO Indoor/Outdoor
MA-WE2458 -3H
http://www.mars-antennas.com/item/023097b0c9b3-179.html

TERRAWAVE 2.4Ghz and 5Ghz 2.5/4dBi Omnidirectional MIMO Indoor
M6025040MO1D3620P
http://www.terra-wave.com/shop/80211n-245-ghz-254-dbi-mini-mimo-ceiling-mount-omnidirectional-antenna-with-plenum-pigtails-and-rpsma-plug-connector-p-1338.html

TERRAWAVE 2.4Ghz and 5Ghz 6dBi Omnidirectional MIMO Outdoor
M6060060MO13620O
http://www.terra-wave.com/shop/80211n-245-ghz-6-dbi-mimo-outdoor-omnidirectional-antenna-with-rpsma-plug-connector-p-919.html

TERRAWAVE 2.4Ghz and 5Ghz 6/7dBi Narrow Beam 82 degree MIMO Indoor/Outdoor M6060070MP13620
http://www.terra-wave.com/shop/80211n-245-ghz-67-dbi-mimo-patch-antenna-with-rpsma-plug-connector-p-922.html

---

**What access points are supported by the vWLAN?**

The vWLAN is built upon 802.11n technology and therefore requires 802.11n BlueSecure access points. The vWLAN supports BSAP-1800v1, BSAP-1800v2, and BSAP-1840 BlueSecure access points. The vWLAN does not support legacy BlueSecure 802.11a/b/g access points i.e. BSAP-1500/1540/1700 or 3rd party access points. BSAP18xx's are backwards compatible to support 802.11a/b/g.

---

**What is the default management IP address of the BSAP?**

192.168.190.1

---

**What is the default serial console and ssh username and password of the BSAP?**

**Username**
adm1n

**Password**
blue1socket

*BSAP-1700 and BSAP-1800v1 do not have serial console ports

---

**What port should I use to access the BSAP CLI via SSH?**

2335

---

**What ports and protocols do I need to allow in the firewall between the BSAP and BSC?**

IP Protocol 97 (EtherIP) - Client Data
TCP/UDP 33333 - Control Channel
UDP 53 - APDiscovery
NAT can NOT be enabled between the BSAP and BSC

---

**What ports and protocols do I need to allow in the firewall between the BSAP and vWLAN?**

IP Protocol 97 (EtherIP) - Client Data (vWLAN 1.0 ONLY)
TCP/UDP 33333 - Control Channel
UDP port 53 (DNS) - APDiscovery
UDP port 69 (TFTP) - Firmware
TCP port 28000 - RFIDS Channel (vWLAN 2.0 ONLY)
TCP port 80 (HTTP) - Only if Web Auth and or Blueprotect are enabled (vWLAN 2.0 ONLY)
TCP port 443 (HTTPS) - Only if Web Auth and or Blueprotect are enabled (vWLAN 2.0 ONLY)
NAT can be enabled between the BSAP and vWLAN

---

**What type of antenna connectors do the BSAP-1840's have?**

The BSAP-1840's have 6 RPSMA-Jack or female connectors (outside thread/inside pin). 3 for the 2.4gHz radio and 3 for the 5gHz radio. They require an antenna with an RPSMA-Plug or male connector (inside thread/inside receptacle)

---

**What type of cable, what terminal emulation settings, and what default username and password is required to connect to the serial console port of the BSAP-1500/1540?**

**Cable**
DB9 9 Pin Null Modem Serial Cable Female/Female

**Terminal Emulation Settings**
Bits per second: 9600
Data bits: 8
Parity: none
Stop bits: 1
Flow control: none

**Username**
adm1n
**Password**
blue1socket

---

**What type of cable, what terminal emulation settings, and what default username and password is required to connect to the serial console port of the BSAP-1800v2/1840?**

**Cable**
DB9 Female to RJ45 Rollover Cable

**Terminal Emulation Settings**
Bits per second: 115200
Data bits: 8
Parity: none
Stop bits: 1
Flow control: none

**Username**
adm1n
**Password**
blue1socket

---

**What type of Power Over Ethernet (POE) is required to power the BSAP?**

The BSAPs are 802.3af class 3 compliant meaning they use up to 15.4 watts. Any switch, injector or midspan which meets these requirements can be used. This includes the BSAP-15XX, 17XX, 18XX however excludes the BSAP-16XX which uses proprietary POE power supply.

---

**When connecting to Bluesocket Access Points with Realtek Wireless Adapter I am able to pass traffic for 2-3 minutes and then I am no longer able to pass any traffic.**

Bluesocket has had several reports of various Realtek Wireless Adapters (rtl8192e, rtl8188ce, rtl8191se) exhibiting these symptoms. Troubleshooting revealed the Realtek Wireless Adapter going into a power save mode (SM Power Save) that is not supported by the AP. The client should not go into this mode unless the AP advertises that it is supported.

In each case, upgrading to the latest Realtek driver sourced directly from Realtek has resolved the issue. Bluesocket has found that some laptop manufacturers, Toshiba for example, have posted outdated drivers that do not include a fix for this issue. Here's the link to download the latest driver directly from Realtek:

http://www.realtek.com.tw/downloads/downloadsView.aspx?Langid=2&PNid=21&PFid=48&Level=5&Conn=4&ProdID=272&DownTypeID=3&GetDown=false&Downloads=true

Bluesocket has identified while some Realtek Wireless Adapters have the fix included in the latest driver, others do not. First try upgrading to the latest driver. If that does not resolve the issue, another work around is to disable 802.11N on the Realtek wireless adapter, until Realtek releases a driver for your adapter with the fix.

---

**Intel 2200BG/2915ABG unable to connect to BSAP or poor performance/disconnects**

Set compatibility mode on the client under advanced wireless adapter properties to CTS/RTS. Please also make sure you have obtained and installed the latest drivers from Intel.

---